

## G14 APPLICATION SYSTEM REVIEWS

The specialised nature of information systems (IS) auditing and the skills necessary to perform such audits require standards that apply specifically to IS auditing. One of the goals of ISACA<sup>®</sup> is to advance globally applicable standards to meet its vision. The development and dissemination of the IS Auditing Standards are a cornerstone of the ISACA professional contribution to the audit community. The framework for the IS Auditing Standards provides multiple levels of guidance:

- **Standards** define mandatory requirements for IS auditing and reporting. They inform:
  - IS auditors of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics
  - Management and other interested parties of the profession's expectations concerning the work of practitioners
  - Holders of the Certified Information Systems Auditor™ (CISA<sup>®</sup>) designation of requirements. Failure to comply with these standards may result in an investigation into the CISA holder's conduct by the ISACA Board of Directors or appropriate ISACA committee and, ultimately, in disciplinary action.
- **Guidelines** provide guidance in applying IS Auditing Standards. The IS auditor should consider them in determining how to achieve implementation of the standards, use professional judgement in their application and be prepared to justify any departure. The objective of the IS Auditing Guidelines is to provide further information on how to comply with the IS Auditing Standards.
- **Procedures** provide examples of procedures an IS auditor might follow in an audit engagement. The procedure documents provide information on how to meet the standards when performing IS auditing work, but do not set requirements. The objective of the IS Auditing Procedures is to provide further information on how to comply with the IS Auditing Standards.

**Control Objectives for Information and related Technology (CobIT<sup>®</sup>)** is an information technology (IT) governance framework and supporting tool set that allow managers to bridge the gaps amongst control requirements, technical issues and business risks. CobIT enables clear policy development and good practice for IT control throughout enterprises. It emphasises regulatory compliance, helps organisations increase the value attained from IT, enables alignment and simplifies implementation of the CobIT framework's concepts.

CobIT is intended for use by business and IT management as well as IS auditors; therefore, its usage enables the understanding of business objectives and communication of good practices and recommendations to be made around a commonly understood and well-respected framework. CobIT is available for download on the ISACA web site, [www.isaca.org/cobit](http://www.isaca.org/cobit). As defined in the CobIT framework, each of the following related products is organised by IT management process:

- **Control objectives**—Generic statements of minimum good control in relation to IT processes
- **Management guidelines**—Guidance on how to assess and improve IT process performance, using maturity models; Responsible, Accountable, Consulted and/or Informed (RACI) charts; goals; and metrics. They provide a management-oriented framework for continuous and proactive control self-assessment specifically focused on:
  - Performance measurement
  - IT control profiling
  - Awareness
  - Benchmarking
- **CobIT<sup>®</sup> Control Practices**—Risk and value statements and 'how to implement' guidance for the control objectives
- **IT Assurance Guide**—Guidance for each control area on how to obtain an understanding, evaluate each control, assess compliance and substantiate the risk of controls not being met

A **glossary** of terms can be found on the ISACA web site at [www.isaca.org/glossary](http://www.isaca.org/glossary). The words audit and review are used interchangeably in the IS Auditing Standards, Guidelines and Procedures.

**Disclaimer:** ISACA has designed this guidance as the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics. ISACA makes no claim that use of this product will assure a successful outcome. The publication should not be considered inclusive of any proper procedures and tests or exclusive of other procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific procedure or test, controls professionals should apply their own professional judgement to the specific control circumstances presented by the particular systems or IT environment.

The ISACA Standards Board is committed to wide consultation in the preparation of the IS Auditing Standards, Guidelines and Procedures. Prior to issuing any documents, the Standards Board issues exposure drafts internationally for general public comment. The Standards Board also seeks out those with a special expertise or interest in the topic under consideration for consultation where necessary. The Standards Board has an ongoing development programme and welcomes the input of ISACA members and other interested parties to identify emerging issues requiring new standards. Any suggestions should be e-mailed ([standards@isaca.org](mailto:standards@isaca.org)), faxed (+1.847. 253.1443) or mailed (address at the end of document) to ISACA International Headquarters, for the attention of the director of research, standards and academic relations. This material was issued 15 October 2008.

### 1. BACKGROUND

## 1.1 Linkage to Standards

- 1.1.1 Standard S6 Performance of Audit Work states 'During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence'.

## 1.2 Linkage to COBIT

- 1.2.1 Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices. To meet the G 14 Application Systems Reviews requirements of IS auditors, the processes in COBIT most likely to be relevant, selected and adapted are classified here as primary and secondary. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

- 1.2.2 Primary IT processes are:

- PO9 *Assess and manage IT risks*
- AI2 *Acquire and maintain application software*
- DS5 *Ensure systems security*
- ME2 *Monitor and evaluate internal control*

- 1.2.3 Secondary IT processes are:

- PO7 *Manage IT human resources*
- PO8 *Manage quality*
- A16 *Manage changes*
- DS3 *Manage performance and capacity*
- DS10 *Manage problems*
- DS11 *Manage data*

- 1.2.4 The information criteria most relevant to application system reviews are:

- Primary: Availability, reliability, integrity and confidentiality
- Secondary: Compliance, effectiveness and efficiency

## 1.3 Need for Guideline

- 1.3.1 The purpose of this guideline is to describe the recommended practices in performing an application systems review.

- 1.3.2 The purpose of an application systems review is to identify, document, test and evaluate the controls over an application that are implemented by an organisation to achieve relevant control objectives. These control objectives can be categorised into control objectives over the system and the related data.

## 2. PLANNING

### 2.1 Planning Considerations

- 2.1.1 An integral part of planning is understanding the organisation's IS environment to a sufficient extent for the IS auditor to determine the size and complexity of the systems and the extent of the enterprise's dependence on information systems. The IS auditor should gain an understanding of the enterprise's mission and business objectives, the level and manner in which information technology and information systems are used to support the enterprise, and the risks and exposures associated with the enterprise's objectives and its information systems. Also, an understanding of the organisational structure including roles and responsibilities of key IS staff and the business process owner of the application system should be obtained.

- 2.1.2 A primary objective of planning is to identify the application-level risks. The relative level of risk influences the level of audit evidence required.

- 2.1.3 Application-level risks at the system and data level include such things as:

- System availability risks relating to the lack of system operational capability
- System security risks relating to unauthorised access to systems and/or data
- System integrity risks relating to the incomplete, inaccurate, untimely or unauthorised processing of data
- System maintainability risks relating to the inability to update the system when required in a manner that continues to provide for system availability, security and integrity

- Data risks relating to its completeness, integrity, confidentiality, privacy and accuracy
- 2.1.4** Application controls to address the application-level risks may be in the form of computerized controls built into the system, manually performed controls, or a combination of both. Examples include the computerized matching of documents (purchase order, invoice and goods received report), the checking and signing of a computer generated cheque and the review by senior management of exception reports.
- 2.1.5** Where the option to place reliance on programmed controls is taken, relevant general IT controls should be considered, as well as controls specifically relevant to the audit objective. General IT controls could be the subject of a separate review, which would include such things as physical controls, system-level security, network management, data backup and contingency planning. Depending on the control objectives of the review, the IS auditor may not need to review general controls, such as where an application system is being evaluated for acquisition.
- 2.1.6** Application system reviews can be performed when a package application system is being evaluated for acquisition, before the application system goes into production (pre-implementation) and after the application system has gone into production (post-implementation). Pre-implementation application system review coverage includes the architecture of application-level security, plans for the implementation of security, the adequacy of system and user documentation, and the adequacy of actual or planned user-acceptance testing. Post-implementation review coverage includes application-level security after implementation and system conversion if there has been a transfer of data and master file information from the old to the new system.
- 2.1.7** The objectives and scope of an application systems review usually form part of the terms of reference. The form and content of the terms of reference may vary but should include:
- The objectives and scope of the review
  - IS auditors performing the review
  - A statement regarding the independence of the IS auditors from the project
  - When the review will commence
  - The time frame of the review
  - Reporting arrangements
  - Closing meeting arrangements
  - Objectives should be developed to address the seven COBIT information criteria and then agreed upon by the enterprise. The seven COBIT information criteria are:
    - Effectiveness
    - Efficiency
    - Confidentiality
    - Integrity
    - Availability
    - Compliance
    - Reliability of information
- 2.1.8** Where the IS auditor has been involved previously in the development, acquisition, implementation or maintenance of an application system and is assigned to an audit engagement, the independence of the IS auditor may be impaired. The IS auditor should refer to appropriate guidelines to deal with such circumstances.

### **3. PERFORMANCE OF AUDIT WORK**

#### **3.1 Documenting the Flow of Transactions**

- 3.1.1** Information gathered should include both the computerized and manual aspects of the system. The focus should be on data input (whether electronic or manual), processing, storage and output that are of significance to the audit objective. The IS auditor may find, depending upon the business processes and the use of technology, that documenting the transaction flow may not be practical. In that event, the IS auditor should prepare a high-level data-flow diagram or narrative and/or utilise system documentation if provided. Consideration should also be given to documenting application interfaces with other systems.
- 3.1.2** The IS auditor may confirm the documentation by performing procedures such as a walk-through test.

## 3.2 Identifying and Testing the Application System Controls

3.2.1 Specific controls to mitigate the application risks may be identified and sufficient audit evidence obtained to assure the IS auditor that the controls are operating as intended. This can be accomplished through procedures such as:

- Inquiry and observation
- Review of documentation
- Testing of the application system controls where programmed controls are being tested. The use of computer-assisted audit techniques (CAATs) may be considered.

3.2.2 The nature, timing and extent of testing should be based on the level of risk to the area under review and the audit objectives. In the absence of strong general IT controls, the IS auditor may make an assessment of the effect of this weakness on the reliability of the computerized application controls.

3.2.3 If the IS auditor finds significant weaknesses in the computerized application controls, assurance should be obtained (depending on the audit objective), if possible, from the manually performed processing controls.

3.2.4 The effectiveness of computerized controls is dependent on strong general IT controls. Therefore, if general IT controls are not reviewed, the ability to place reliance on the application controls may be limited severely and the IS auditor should consider alternative procedures.

## 4. REPORTING

### 4.1 Weaknesses

4.1.1 Weaknesses identified in the application review either due to an absence of controls or to non-compliance should be brought to the attention of the business process owner and to the IS management responsible for the support of the application. Where weaknesses identified during the application systems review are considered to be significant or material, the appropriate level of management should be advised to undertake immediate corrective action.

4.1.2 Since effective computerised application controls are dependent on general IT controls, weaknesses in this area should also be reported. In the event that general IT controls were not reviewed, this fact should be included in the report.

4.1.3 The IS auditor should include appropriate recommendations to strengthen controls in the report.

## 5. EFFECTIVE DATE

5.1 This guideline is effective for all IS audits beginning on or after 1 November 2001. The guideline has been reviewed and updated effective 1 December 2008.

### 2008-2009 ISACA Standards Board

Chair, Ravi Muthukrishnan, CISA, CISM, FCA, ISCA	Capco IT Services India Private Ltd., India
Shawn Chaput, CISA, CISM, CISSP, PMP	IBM, Canada
Maria Gonzalez, CISA, CISM	Department of Defence, Spain
John Ho Chi, CISA, CISM, CBCP, CFE	Ernst & Young, Singapore
Andrew J. MacLeod, CISA, FCPA, MACS, PCP, CIA	Brisbane City Council, Australia
John G. Ott, CISA, CPA	AmerisourceBergen, USA
Edward Pelcher, CISA	Office of the Auditor General, South Africa
Jason Thompson, CISA	KPMG LLP, USA
Meera Venkatesh, CISA, CISM, ACS, CISSP, CWA	Microsoft Corp., USA

ISACA  
3701 Algonquin Road, Suite 1010  
Rolling Meadows, IL 60008 USA  
Telephone: +1.847.253.1545  
Fax: +1.847.253.1443  
E-mail: [standards@isaca.org](mailto:standards@isaca.org)  
Web Site: [www.isaca.org](http://www.isaca.org)